Desarrollo Seguro

Lección 4: Auditando y securizando.

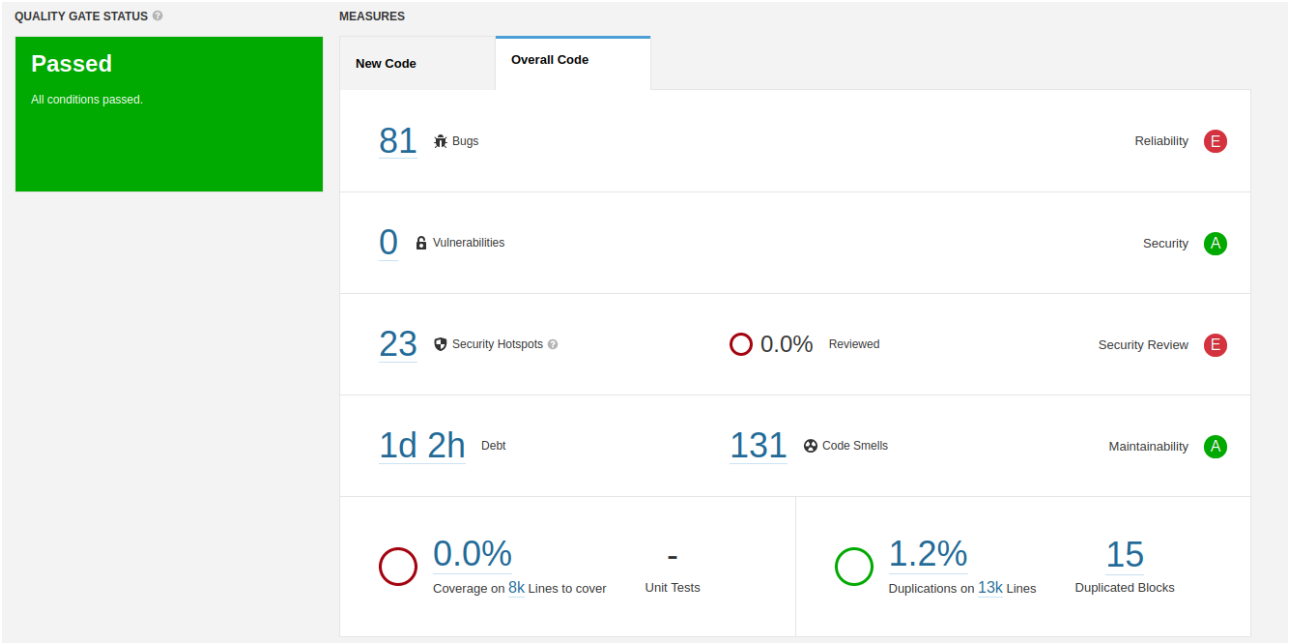
eip ESCUELA INTERNACIONAL POSGRADOS

Indice

Introducción

EN la presente lección se han explicado varias herramientas empleadas en la securización y auditorización de código con la que se pide realizar una auditoria a un programa y en función del resultado exponer y justificar las acciones correctivas a tomar teniendo en cuenta OWASP

L4_DS_django_shop



Security Hotspots

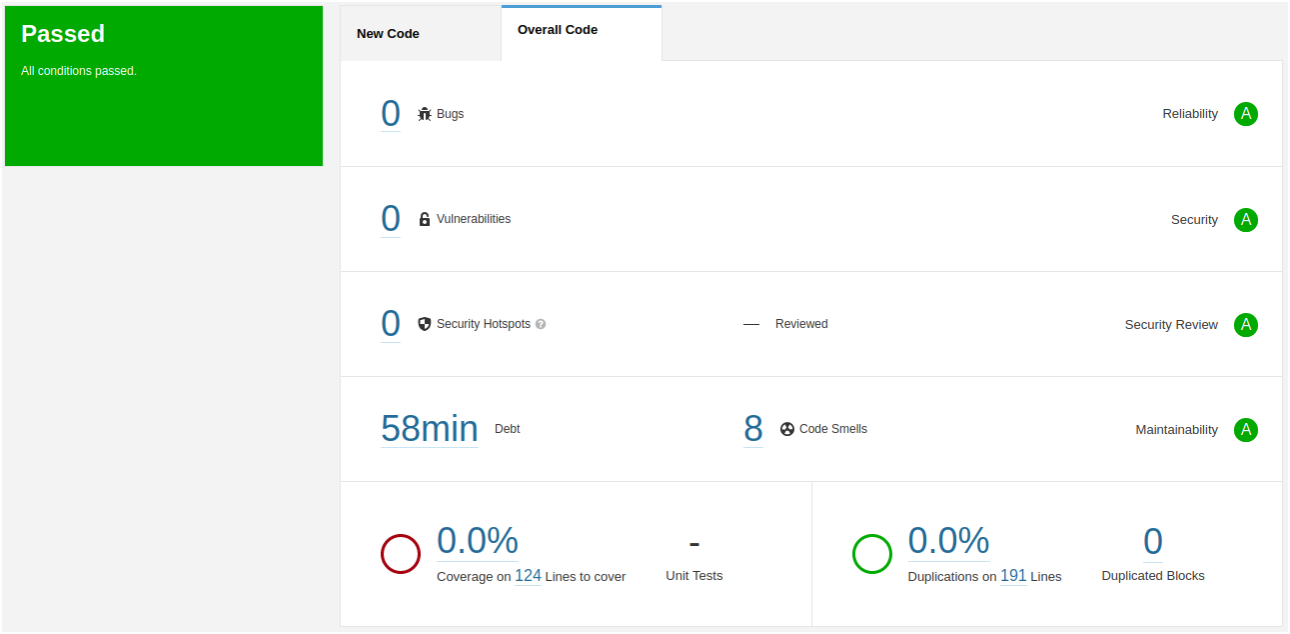
Authentication

El código presenta 21 hotspot en los que la contraseña ha sido herdcodeada, estos elementos generan un punto de acceso de alto riesgo y pueden provocar vectores de ataque del tipo Perdida de Autenticación para evitarlo habría que aplicar un cifrado a las contraseñas de modo que no sean legibles desde el exterior o emplear código que proteja este tipo de información.

Insecure Configuration

El código también presenta un problema del tipo Insecure configuration, esto se soluciona estableciendo el Debug a False una vez el código pase a producción, de otro modo, esto podría generar problemas de tipo exposición de datos sensibles , perdida de control de acceso etc ya que al darse un error podría mostrase lineas de código aprovechables en un ataque.

L4_DS_gastos



Security Hotsopts

Por otra parte, el código desarrollado en el máster que ha sido sometido a la auditoria, no presenta ningún Hotspot, esto se debe a que se trata de un código muy sencillo que únicamente pretende analizar un csv con la finalidad de obtener cierta información. Sin embargo ya que se trata de un programa que en teoría maneja información financiera y privada habría que aplicarle ciertos controles pro-activos como pueden ser Acceso seguro a la base de datos para evitar ataques del tipo inyección de sql, validación de las entradas para evitar que se puedan introducir lineas de código maliciosas y aplicar controles de acceso para limitar la posibilidad de que suceda un robo de información.